Docket No. AUS920010386US1 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Arbab et al.**	§	
	§	Group Art Unit: **2132**
Serial No. **09/909,251**	§	
	§	Examiner: **Minh Dinh**
Filed: **July 19, 2001**	§	
	§	
For: **Apparatus and Method for Multi-Threaded Password Management**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on November 20, 2006.

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation of Armonk, New York.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-32.

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 6, 7 and 30.
2. Claims withdrawn from consideration but not canceled: None.
3. Claims pending: 1-5, 8-29, 31 and 32.
4. Claims allowed: None.
5. Claims rejected: 1-5, 8-29, 31 and 32.
6. Claims objected to: None.

C. CLAIMS ON APPEAL

The claims on appeal are: 1-5, 8-29, 31 and 32.

STATUS OF AMENDMENTS

No amendment after final was filed for this case.

SUMMARY OF CLAIMED SUBJECT MATTER

Generally speaking, the claims of this application are directed to a multi-threaded password management system where passwords for a plurality of different resources that are accessible by a user may be grouped together. When a user initiates the changing of one of the resource's passwords in a group, the other resources in the group can also automatically be changed in response to the change to the first password being changed to thereby facilitate a reduction in the amount of effort required to periodically update a plurality of passwords. To assist in such user actions, the user is provided with a listing of resources that includes *a display that indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources* such that the user does not have to manually make this determination.

A. CLAIM 1 - INDEPENDENT

Claim 1 is directed to a method of managing resource passwords for resources organized into a plurality of groups of resources. A user is provided with a listing of resources to which the user is given access. This step of providing the user with a listing of resources includes providing the user with *a display that indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources.* Selections are received from the user for grouping various ones of the resources into groups of resources. The plurality of groups of resources are stored in a user password profile. A plurality of resources that are part of a group of resources are identified by retrieving the user password profile in which the plurality of groups of resources are identified along with corresponding group password information for each of the plurality of groups of resources. A first password for a first resource in the group of resources is updated. A second password for a second resource in the group of resources is updated based on the updating of the first password for the first resource (Specification page 9, line 11 – page 11, line 10; page 15, line 3 – page 17, line 8; Figures 5 and 6, all blocks).

B. CLAIM 18 - INDEPENDENT

Claim 18 is directed to a computer program product tangibly embodied in a tangible computer readable medium for managing resource passwords for resources organized into a plurality of groups of resources. First instructions are provided for identifying a plurality of resources that are part of a group of resources, by retrieving a user password profile in which the plurality of groups of resources are identified along with corresponding group password information for each of the plurality of groups of resources. Each of the plurality of groups of resources is a group of resources which use the same password to authenticate a user's access to the resource. Second instructions are provided for updating a first password for a first resource in the group of resources. Third instructions are provided for updating a second password for a second resource in the group of resources based on the updating of the first password for the first resource, wherein the second password is updated automatically without user intervention (Specification page 9, line 11 – page 11, line 10; page 15, line 3 – page 17, line 8; Figures 5 and 6, all blocks).

C. CLAIM 31 - INDEPENDENT

Claim 31 is directed to an apparatus for managing resource passwords. The apparatus includes means for providing a user with a listing of resources to which the user is given access, including providing the user with *a display that indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources*. The apparatus also includes means for identifying a plurality of resources that are part of a group of resources. The group of resources is a group of resources each of which use the same password to authenticate a user's access to a resource defined to the group of resources. The apparatus also includes means for updating a first password for a first resource in the group of resources. The apparatus also includes means for updating a second password for a second resource in the group of resources based on the updating of the first password for the first resource (Specification page 9, line 11 – page 11, line 10; page 15, line 3 – page 17, line 8; Figures 5 and 6, all blocks).

The structure corresponding to each of the above listed means (means for providing, means for identifying, means for updating a first password and means for updating a second password) is described at Specification page 13, line 2 – page 15, line 2 as depicted in Figure 4).

D. CLAIM 32 - INDEPENDENT

Claim 32 is directed to a method of managing resource passwords. *A plurality of resources that may be grouped together are identified according to non-password security parameters associated with the plurality of resources.* A selection of two or more of the plurality of resources to be grouped together in a family of resources is received. A first password for a first resource in the family of resources is updated. A second password for a second resource in the family of resources is updated based on the updating of the first password (Specification page 9, line 11 – page 11, line 10; page 15, line 3 – page 17, line 8; Figures 5 and 6, all blocks).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to review on appeal are as follows:

1. Whether the rejection of Claims 18-29 under 35 U.S.C. §112, first paragraph as failing to comply with the written description requirement is proper;

2. Whether Claims 1-4, 8-21, 23-29 and 31-32 are obvious over *Randall* ("ManageYour Passwords") in view of *Parker* ("P-Synch") under 35 U.S.C. §103; and

3 Whether Claims 5 and 12 are obvious over *Parker* ("P-Synch") in view of *Stallings* ("Operating Systems – Internal and Design Principles") under 35 U.S.C. §103.

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 18-29)

A.1. Claims 18-29

As an initial matter, it should be noted that these Claims 18-29 have been erroneously rejected as failing to comply with the *written description* requirement. It is the Specification, and *not* the claims, that must comply with the written description requirement of 35 USC §112, 1st paragraph[1], and thus the reasons given in rejecting Claims 18-29 (the *claims* do not comply with the written description requirement) is clearly erroneous.

Still further, the Examiner states that the limitation "tangible" that was added to the claim was not disclosed in the originally filed specification. Appellants urge error, in that the Specification describes at page 17, beginning on line 17:

> "It is important to note that while the present invention has been described in the context of a fully functioning data processing system, those of ordinary skill in the art will appreciate that the processes of the present invention are capable of being distributed in the form of a computer readable medium of instructions and a variety of forms and that the present invention applies equally regardless of the particular type of signal bearing media actually used to carry out the distribution. Examples of computer readable media include recordable-type media such a floppy disc, a hard disk drive, a RAM, and CD-ROMs and transmission-type media such as digital and analog communications links."

As can be seen, the Specification does in fact describe numerous examples of different types of tangible media for which the computer program product can be tangibly embodied on. Applicants are entitled to generalize their claim to recite a 'genus' type of element instead of individually listing all detailed 'species', and such practice does not constitute new matter

---

[1] The **specification** shall contain a **written description** of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

pursuant to *Bilstad v. Wakalopulos* (03-1528, Fed. Cir. 2004)[2], since the specification clearly conveys to one skilled in the art that the processes of the present invention are capable of being distributed in the form of a computer program product tangibly embodied in a tangible computer readable medium (also see *In re Rasmussen*, 650 F.2d 1212, 1215 (CCPA 1981) where the court explained: "[T]hat a claim may be broader than the specific embodiment disclosed in a specification is in itself of no moment, and *In re Smythe*, 480 F.2d 1376, 1382 (CCPA 1973), where use of the term 'inert fluid' was proper in the claim even though the word 'fluid' did not appear in the Specification).

Thus, at least for the two reasons given above, Claims 18-29 have been erroneously rejected under 35 U.S.C. §112, first paragraph as failing to comply with the written description requirement.

B. GROUND OF REJECTION 2 (Claims 1-4, 8-21, 23-29 and 31-32)

B.1. Claims 1-4, 8-15, 17-21, 23-29 and 31

Claims 1-4, 8-15, 17-21, 23-29 and 31 were rejected under 35 USC §103 as being obvious over *Randall* in view of *Parker*.

With respect to Claim 1, such claim recites "providing a user with a listing of resources to which the user is given access, wherein providing the user with a listing of resources includes providing the user with a display that indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources; and receiving selections from the user for grouping various ones of the resources into groups of resources". As can be seen, the user is provided with a display that indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources. The cited *Randall* reference describes a password management utility named Critical Mass. This utility is described as being used to manage one or more databases that store multiple user passwords to assist a user in managing their plurality of passwords to different resources such as applications, remote systems and web pages. In addition, the different resources are organized into high-level categories such as Applications, Remote Systems, Serial Numbers, Wallet, Web

[2] This court has continued to apply the rule that disclosure of a species may be sufficient written description support for a later claimed genus including that species.

Pages, and Miscellaneous. When adding new information, a user invokes an Add Entry Wizard which presents a user with a display where they can select one of the above listed categories, and the user is then presented with a screen containing multiple labeled fields (which are blank) associated with the selected category that the user can then manually enter appropriate information (such as the name of the application, username, password and name of the file that launches the application; *Randall*, 5th paragraph, last sentence). The cited *Parker* reference provides an automated procedure such that each of a plurality of resources can be individually accessed to change a password from a single location (page 1, last paragraph; page 2, first full paragraph; page 2, last paragraph).

A primary issue in the rejection of Claim 1 is whether any of the cited references teach or suggest the claimed feature of "providing a user with a listing of resources to which the user is given access", which includes "providing the user with a *display that indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources*". From the cursory description of the Critical Mass utility program provided by the cited *Randall* reference, the user is merely presented with a particular wizard based upon which one of a plurality of different standard, generic categories is displayed to and selected by a user, and once the user selects one of such 'canned' categories, certain predefined, and empty/blank fields are presented to the user for manual entry. For example, and importantly, the user must manually input the application name for a given application (*Randall*, 5th paragraph, last sentence). In contrast, and per the features of Claim 1, the *system itself* gathers the potential resources in order to provide the user with a display that *indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources.* The user then groups the resources together per the features of Claim 1. The issue thus becomes whether a display of pre-existing, generic categories for user selection teaches/suggests displaying an indication of *which* of the resources may be grouped together *based upon non-password security parameters associated with the resources.* It is respectfully urged that this is not the case. For example, the *Randall* generic categories are not resources having passwords, but instead are a classification system – and associated names for each of the classification categories – for which underlying resources and associated passwords can be organized (*Randall* 4th paragraph). Importantly, this display of categories provides no information as to the

underlying resources and associated passwords, and this display of categories provides no information as to which resources *may be grouped together based upon non-password security parameters associated with the resources*. This distinction can also be seen due to the fact that these *Randall* categories do not have security parameters associated with them, as they are mere classification buckets (*Randall*, 4th paragraph). In contrast, Claim 1 expressly states that there are security parameters associated with the resources. Therefore, *Randall's* categories, and the display thereof, are very different from the claimed resources and the associated *display that indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources*. Quite simply, the cited *Randall* reference teaches that a user selects a category – which is different from the claimed resources – and then the user is presented with blank fields where the *user manually provides details for resources and their associated passwords*. The cited *Parker* reference does not overcome this teaching/suggestion deficiency. Thus, Claim 1 has been erroneously rejected as being obvious in view of the cited references, as there are missing claimed features (such as to provide the user with a display that *indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources*) not taught or suggested by any of the cited references.

B.2. Claim 16

Claim 16 was rejected under 35 USC §103 as being obvious over *Randall* in view of *Parker*.

In addition to the reasons given above with respect to Claim 1 (of which Claim 16 depends upon), Appellants further urge error in the rejection of Claim 16, as such claim recites that the *user password profile is distributed across the resources*. In rejecting Claim 16, the Examiner only alleges that the *password synchronization utility* program can be run on any machine on the network per the teachings of *Parker*. However, a close review of the *Parker* discussion regarding use of information/files on multiple devices/resources merely states that *the password to be changed* is stored on such remote devices (*Parker* page 2, 1st full paragraph). This information could not reasonably be construed to be the claimed 'user password profile' since Claim 1 (of which Claim 16 depends upon) states that such password profile is used *during group identification* ("identifying a plurality of resources that are part of a group of resources by

retrieving the user password profile in which the plurality of groups of resources are identified along with corresponding group password information for each of the plurality of groups of resources"). Even if one were to construe the individual password files to be a part of the password profile, *Parker* makes no mention that this *profile information is retrieved in order to identify a plurality of resources that are a part of a group of resources*, as per Claim 16 in combination with Claim 1. Thus, a proper *prima facie* showing of obviousness has not been established with respect to Claim 16[3], and accordingly Claim 16 has been erroneously rejected[4].

B.3. Claim 32

Claim 32 was rejected under 35 USC §103 as being obvious over *Randall* in view of *Parker*.

With respect to Claim 32, such claim recites "identifying a plurality of resources that may be grouped together according to non-password security parameters associated with the plurality of resources". As can be seen, a *plurality of resources that may be grouped together is identified according to non-password security parameters associated with the plurality of resources*. The *Randall* reference, cited as teaching this claimed step, instead merely states:

> The databases can contain any type of private information, which you classify using the program's categories: Applications, Remote systems, Serial numbers, Wallet, Web pages, or Miscellaneous. These categories let you store the serial numbers and CD keys for your programs (ever try to reinstall MS Office without the CD key?), the passwords for opening your applications, the usernames and passwords for access to remote systems" (*Randall*, 4th paragraph).

As can be seen, this reference merely describes – with respect to the described categories - that a *user can manually classify* entries within these category buckets. This discussion does not teach or otherwise suggest any type of ability for "identifying a plurality of resources that may be grouped together according to non-password security parameters associated with the plurality of

[3] To establish *prima facie* obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03. *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974).

[4] If the examiner fails to establish a *prima facie* case, the rejection is improper and will be overturned. *In*

resources", as described in detail above with respect to Claim 1. Thus, as there are missing claimed features that are not taught or suggested by the cited reference ("identifying a plurality of resources that may be grouped together according to non-password security parameters associated with the plurality of resources"), it is urged that Claim 32 is not obvious in view of the cited references.

C. GROUND OF REJECTION 3 (Claims 5 and 22)

C.1. Claims 5 and 22

Claims 5 and 22 were rejected under 35 USC §103 as being obvious over *Parker* in view of *Stallings*.

With respect to Claim 5, it is urged that neither one of the cited *Parker* or *Stallings* references teaches or suggests the claimed feature of "a display that indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources", as recited in Claim 1 (of which Claim 5 depends upon)[5]. Therefore, as there are missing claimed features not taught or suggested by any of the cited references, it is urged that Claims 5 and 22 have been erroneously rejected under 35 U.S.C. §103 as being obvious over *Parker* ("P-Synch") in view of *Stallings* ("Operating Systems – Internal and Design Principles").

Appellants have thus shown numerous and substantial error in the Examiner's final rejection of all pending claims, and thus respectfully request that the Board reverse all such claim rejections.

/Wayne P. Bailey/
Wayne P. Bailey
Reg. No. 34,289
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

---

re Fine, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

[5] In rejecting Claim 1, the *Randall* reference was cited as allegedly teaching this claimed feature, but *Randall* is not being used as a reference in this 35 USC §103 rejection of Claim 5.

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method of managing resource passwords for resources organized into a plurality of groups of resources, comprising:

providing a user with a listing of resources to which the user is given access, wherein providing the user with a listing of resources includes providing the user with a display that indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources;

receiving selections from the user for grouping various ones of the resources into groups of resources;

storing the plurality of groups of resources in a user password profile;

identifying a plurality of resources that are part of a group of resources by retrieving the user password profile in which the plurality of groups of resources are identified along with corresponding group password information for each of the plurality of groups of resources;

updating a first password for a first resource in the group of resources; and

updating a second password for a second resource in the group of resources based on the updating of the first password for the first resource.

2. The method of claim 1, wherein the first password and the second password are the same.

3. The method of claim 1, wherein updating a second password for a second resource in the group of resources includes updating passwords for each of the resources in the group of resources to be the same as the first password.

4. The method of claim 1, wherein updating the first password for the first resource and updating the second password for the second resource are both performed in response to determining that the first password is about to expire.

5. The method of claim 1, wherein at least one process spawns threads to update the first password and second password in response to updating the group password information.

8. The method of claim 1, wherein providing the user with a listing of resources includes providing the user with a display that indicates which of the resources are already grouped with one another.

9. The method of claim 1, further comprising:

storing a password in association with each of the groups of resources, wherein the password is used with each of the resources in a corresponding group of resources.

10. The method of claim 1, wherein updating a second password for a second resource in the group of resources includes updating only selected ones of the resources in the group of resources.

11. The method of claim 1, wherein updating a second password for a second resource in the group of resources includes:

prompting a user to change a password for one or more of the resources in the group of resources; and

changing the password for the one or more resources selected by the user.

12. The method of claim 11, wherein the one or more resources selected by the user includes all of the resources in the group of resources.

13. The method of claim 1, wherein the group of resources is a group of resources each of which use the same password to authenticate a user's access to the resource

14. The method of claim 1, wherein the user password profile is stored on a server.

15. The method of claim 1, wherein the user password profile is stored on a client device.

16. The method of claim 1, wherein the user password profile is distributed across the resources.

17. The method of claim 1, wherein updating the second password is performed automatically.

18. A computer program product tangibly embodied in a tangible computer readable medium for managing resource passwords for resources organized into a plurality of groups of resources, comprising:

first instructions for identifying a plurality of resources that are part of a group of resources, by retrieving a user password profile in which the plurality of groups of resources are identified along with corresponding group password information for each of the plurality of groups of resources, wherein each of the plurality of groups of resources is a group of resources which use the same password to authenticate a user's access to the resource;

second instructions for updating a first password for a first resource in the group of resources; and

third instructions for updating a second password for a second resource in the group of resources based on the updating of the first password for the first resource, wherein the second password is updated automatically without user intervention.

19. The computer program product of claim 18, wherein the first password and the second password are the same.

20. The computer program product of claim 18, wherein the third instructions for updating a second password for a second resource in the group of resources include instructions for updating passwords for each of the resources in the group of resources to be the same as the first password.

21. The computer program product of claim 18, wherein the second instructions for updating the first password for the first resource and the third instructions for updating the second password for the second resource are both executed in response to determining that the first password is about to expire.

22. The computer program product of claim 18, wherein at least one process spawns threads to update the first password and second password in response to updating the group password information.

23. The computer program product of claim 18, wherein the first instructions include:

instructions for providing a user with a listing of resources to which the user is given access;

instructions for receiving selections from the user for grouping various ones of the resources into the plurality of groups of resources; and

instructions for storing the plurality of groups of resources in the user password profile.

24. The computer program product of claim 23, wherein the instructions for providing the user with a listing of resources include instructions for providing the user with a display that indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources.

25. The computer program product of claim 23, wherein the instructions for providing the user with a listing of resources include instructions for providing the user with a display that indicates which of the resources are already grouped with one another.

26. The computer program product of claim 23, further comprising:

instructions for storing a password in association with each of the groups of resources, wherein the password is used with each of the resources in a corresponding group of resources.

27. The computer program product of claim 18, wherein the third instructions for updating a second password for a second resource in the group of resources include instructions for updating only selected ones of the resources in the group of resources.

28. The computer program product of claim 18, wherein the third instructions for updating a second password for a second resource in the group of resources include:

instructions for prompting a user to change a password for one or more of the resources in the group of resources; and

instructions for changing the password for the one or more resources selected by the user.

29. The computer program product of claim 27, wherein the one or more resources selected by the user includes all of the resources in the group of resources.

31. An apparatus for managing resource passwords, comprising:

means for providing a user with a listing of resources to which the user is given access,

wherein providing the user with a listing of resources includes providing the user with a display that indicates which of the resources may be grouped together based upon non-password security parameters associated with the resources;

means for identifying a plurality of resources that are part of a group of resources, wherein the group of resources is a group of resources each of which use the same password to authenticate a user's access to a resource defined to the group of resources;

means for updating a first password for a first resource in the group of resources; and

means for updating a second password for a second resource in the group of resources based on the updating of the first password for the first resource.

32. A method of managing resource passwords, comprising:

identifying a plurality of resources that may be grouped together according to non-password security parameters associated with the plurality of resources;

receiving a selection of two or more of the plurality of resources to be grouped together in a family of resources;

updating a first password for a first resource in the family of resources; and

updating a second password for a second resource in the family of resources based on the updating of the first password.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.